



# CVE-2022-41184

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-41184
<b>State</b>	PUBLIC
<b>Assigner</b>	cna@sap.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-10-11 21:15:00 UTC
<b>Updated</b>	2023-07-10 21:15:00 UTC
<b>Description</b>	Due to lack of proper memory management, when a victim opens a manipulated Windows Cursor File (.cur, ico.x3d) file rec

## Risk And Classification

**Problem Types:** CWE-119 | CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	3d Visual Enterprise Author	9.0	All	All	All

## References

Reference	Source	Link	Tags
Access Denied	MISC	<a href="http://www.sap.com">www.sap.com</a>	
launchpad.support.sap.com	MISC	<a href="http://launchpad.support.sap.com">launchpad.support.sap.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)